CLAIMS

1. A method of authenticating a data set of a casino-type viewable game, said method comprising the steps of:

(a) providing a data set for a casino game;

(b) computing a first abbreviated bit string unique to the data set;

(c) encrypting the abbreviated bit string to provide a signature;

(d) storing the data set and the signature;

(e) computing a second abbreviated bit string from the stored data set;

(f) decrypting the stored signature to recover the first abbreviated bit string; and

(g) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

2. The method of claim 1 wherein said step (b) of computing is performed with a hash function to produce a hash value of the date set, and wherein said first abbreviated bit string comprises the hash value of the data set.

3. The method of claim 2 wherein the hash value comprises the message digest of the data set.

4. The method of claim 1 wherein said step (c) of encrypting is performed using a private encryption key.

5. The method of claim 1 wherein said step (f) of decrypting is performed using a public decryption key.

6. The method of claim 1 wherein said step (c) of encrypting is performed using a private encryption key, and said step (f) of decrypting is performed using a public decryption key.

7. The method of claim 1 wherein said step (e) of computing is performed with a hash function to produce a hash value of the stored data set, and wherein said second abbreviated bit string comprises the hash value of the stored data set.

8. The method of claim 7 wherein the hash value comprises the message digest of the stored data set.

9. The method of claim 1 wherein said step (d) of storing includes the step of storing the data set and the signature in a mass storage device.

10. The method of claim 9 wherein the mass storage device comprises a disk drive unit.

11. The method of claim 9 wherein the mass storage device comprises a CD-ROM unit.

12. The method of claim 9 wherein the mass storage a network storage system.

13. The method of claim 1 wherein said steps (a)-(d) a first site, and wherein steps (e)-(g) are performed at a second site.

14. The method of claim 13 wherein the first site comprises a manufacturing facility, and wherein said second site is a gaming facility.

15. A method of preparing a casino game data set capable of authentication, said method comprising the steps of:

(a) providing a data set for a casino game;

(b) computing a first abbreviated bit string unique to the casino game data set;

(c) encrypting the abbreviated bit string to provide a signature; and

(d) storing the casino game data set and the signature.

16. The method of claim 15 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game data set, and wherein said first abbreviated bit string comprises the hash value of the stored casino game data set.

17. The method of claim 16 wherein the hash value comprises the message digest of the casino game data set.

18. The method of claim 15 wherein said step (c) of encrypting is performed using a private encryption key.

19. The method of claim 15 wherein said step (d) of step of storing the casino game data set and the signature in a mass storage device.

20. The method of claim 19 wherein the mass storage device comprises a disk drive unit.

21. The method of claim 19 wherein the mass storage device comprises a CD-ROM unit.

22. The method of claim 19 wherein the mass storage device comprises a network storage system.

23. A method of authenticating a casino game data set of a casino type viewable game having a signature encrypted from a first abbreviated bit string computed from the casino game data set, said method comprising the steps of:

(a) computing a second abbreviated bit string from the casino game data set;

(b) decrypting the signature to recover the first abbreviated bit string; and

(c) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

24. The method of claim 23 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game data set, and wherein said second abbreviated bit string comprises the hash value of the casino game data set.

25. The method of claim 24 wherein the hash value comprises the message digest of the casino game data set.

26. The method of claim 23 wherein said step (b) of decrypting is performed using a public decryption key.

27. An electronic gaming system for providing authentication of a data set of a casino type game, said system comprising:

first means for storing a casino game data set and a signature of said casino game data set, said signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game data set;

second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game data set stored in said first storing means and capable of decrypting an encrypted signature stored in said first storing means to recover the first abbreviated bit string;

processing means for enabling the authentication program to compute an abbreviated bit string from the casino game data set stored in said first storing means and for enabling the authentication program to decrypt the encrypted signature stored in said first storing means to provide a decrypted abbreviated bit string; and

means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present.

28. The system of claim 27 wherein said first storing means comprises a mass storage device.

29. The system of claim 28 wherein said mass storage device comprises a disk drive unit.

30. The system of claim 28 wherein said mass storage device comprises a CD-ROM unit.

31. The method of claim 28 wherein said mass storage device comprises a network storage unit.

32. The system of claim 27 wherein said second storing means comprises a read only memory device.

33. The system of claim 32 wherein said read only memory device comprises an unalterable memory device.

34. The system of claim 32 wherein said read only memory device includes a first portion for storing that portion of said authentication program capable of computing the abbreviated bit string from the casino game data set, and a second portion for storing that part of the authentication program capable of decrypting the encrypted signature.

35. The system of claim 34 wherein said second ROM portion is used to store a decryption key.

36. For use in authenticating a casino game data set and signature encrypted from an original message digest computed from the casino game data set; an unalterable read only memory device having stored therein a message digest computing program corresponding to the message digest program used to compute the original message digest of the casino game data set, and a decryption program and decryption key corresponding to the encryption program and encryption key used to prepare the encrypted signature of the original message digest.

37. The device of claim 36 wherein the message digest computing program comprises a hash function.

38. The device of claim 36 wherein the stored decryption key comprises a public key.

39. The device of claim 36 further including an initial loader program stored in said unalterable read only memory device for ensuring use of the message digest computing program, the decryption program and the decryption key.

40. A method of preparing casino game software information capable of authentication, said method comprising the steps of:

(a) providing software information relating to a casino game;

(b) computing a first abbreviated bit string unique to the casino game software information;

(c) encrypting the abbreviated bit string to provide a signature; and

(d) storing the casino game software information and the signature.

41. The method of claim 40 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game software information, and wherein said first abbreviated bit string comprises the hash value of the stored casino game software information.

42. The method of claim 41 wherein the hash value comprises the message digest of the casino game software information.

43. The method of claim 40 wherein said step (c) of encrypting is performed using a private encryption key.

44. The method of claim 40 wherein said step (d) of storing includes the step of storing the casino game software information and the signature in a memory device.

45. A method of authenticating casino game software information having a signature encrypted from a first abbreviated bit string computed from the casino game software information, said method comprising the steps of:

(a) computing a second abbreviated bit string from the casino game software information;

(b) decrypting the signature to recover the first abbreviated bit string; and

(c) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

46. The method of claim 45 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game software information, and wherein said second abbreviated bit string comprises the hash value of the casino game software information.

47. The method of claim 46 wherein the hash value comprises the message digest of the casino game software information.

48. The method of claim 45 wherein said step (b) of decrypting is performed using a public decryption key.

49. An electronic gaming system for providing authentication of software information relating to a casino type game, said system comprising:

first means for storing casino game software information and a signature of said casino game software information, said signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game software information;

second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game software information stored in said first storing means and capable of decrypting an encrypted signature stored in said first storing means to recover the first abbreviated bit string;

processing means for enabling the authentication program to compute an abbreviated bit string from the casino game software information stored in said first storing means and for enabling the authentication program to decrypt the encrypted signature stored in said first storing means to provide a decrypted abbreviated bit string; and means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present.

50. The system of claim 49 wherein said first storing means comprises a memory device.

51. The system of claim 50 wherein said memory device comprises a read only memory.

52. The system of claim 50 wherein said memory device comprises a RAM.

53. The system of claim 49 wherein said second storing means comprises a read only memory device.

54. The system of claim 53 wherein said read only memory device comprises an unalterable memory device.

55. The system of claim 53 wherein said read only memory device includes a first portion for storing that portion of said authentication program capable of computing the abbreviated bit string from the casino game software information, and a second portion for storing that part of the authentication program capable of decrypting the encrypted signature.

56. The system of claim 53 wherein said second ROM portion is used to store a decryption key.

57. The system of claim 49 wherein said casino game software information comprises program information.

58. The system of claim 49 wherein said casino game software information comprises a fixed data set.

59. For use in authenticating casino game software information and a signature encrypted from an original message digest computed from the casino game software information; an unalterable read only memory device having stored therein a message digest computing program corresponding to the message digest program used to compute the original message digest of the casino game software information, and a decryption program and decryption key corresponding to the encryption program and encryption key used to prepare the encrypted signature of the original message digest.

60. The device of claim 59 wherein the message digest computing program comprises a hash function.

61. The device of claim 59 wherein the stored decryption key comprises a public key.

62. The device of claim 59 further including an initial loader program stored in said unalterable read only memory device for ensuring use of the message digest computing program, the decryption program and the decryption key.

Add A'